



---

## **POLICY DOCUMENT**

### **Data Protection Policy**

Document no:	9.0.2019
Version:	4.0
Responsible:	General Counsel ("GC")
Approved by Board of Directors on:	31 October 2019

# DATA PROTECTION POLICY

## Table of Contents

1. BACKGROUND AND PURPOSE .....	1
2. AUDIENCE .....	1
3. SCOPE .....	1
4. POLICY STATEMENT.....	1
5. DEFINITIONS .....	2
6. PRINCIPLES FOR PROCESSING OF PERSONAL DATA .....	2
6.1 <i>Lawfulness, fairness and transparency</i> .....	2
6.2 <i>Purpose limitation and data minimisation</i> .....	3
6.3 <i>Accuracy</i> .....	3
6.4 <i>Storage limitation</i> .....	3
6.5 <i>Integrity and confidentiality</i> .....	3
7. DATA SUBJECT RIGHTS .....	4
8. LEGAL BASIS .....	5
9. DATA PROTECTION RISKS .....	6
10. ROLES AND RESPONSIBILITIES .....	6
11. EXCEPTIONS.....	7
12. REVIEWS AND UPDATES.....	7
13. REFERENCES TO ASSOCIATED DOCUMENTS AND LINKS.....	7

## 1. BACKGROUND AND PURPOSE

Catena Media plc (the "**Company**") and its wholly-owned subsidiaries (jointly referred to as the Catena Group) need to gather and use certain information about individuals. This can include customers, suppliers, business contacts, consultants, freelancers, employees and other people with whom the Catena Group has a relationship with or may need to contact.

This Data Protection Policy (the "**Policy**") for the Catena Group has been developed with the aim of ensuring that the Catena Group:

- Complies with data protection laws and follows good practice
- Creates a framework for cross-border data transmissions within the Catena Group
- Protects the data protection rights and freedom of individuals
- Shows transparency about collection and processing of personal data
- Prevents and manages risks of a data breach
- Is a trustworthy business partner and an attractive employer.

## 2. AUDIENCE

This Policy applies to all directors, employees (including interns, apprentices, trainees), independent contractors, Founders on earn-out and other similarly contracted workers (collectively known as "Relevant Persons").

## 3. SCOPE

This Policy includes accepted data protection principles and supplements the applicable data protection laws and regulations in each relevant country where a Catena Group company carries out business. The relevant national law will take precedence in the event that it conflicts with this Policy, or it has stricter requirements.

These rules apply regardless of whether personal data is stored electronically, on paper or on other materials.

In addition to this Policy, the Catena Group has developed, and will continue to develop when needed, supporting documents (e.g. procedures and instructions) addressing various privacy and data protection matters.

## 4. POLICY STATEMENT

This Policy is applicable whenever processing of personal data takes place within the Catena Group.

## 5. DEFINITIONS

"**applicable laws**" means all legislation and regulations (including those issued by competent supervisory authorities) protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data that from time to time apply the Catena Group, including Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation, GDPR).

"**Catena Media**" means the relevant Catena Group company.

"**data breach**" is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

"**data controller**" is the legally independent company of the Catena Group who decides the purpose and use of personal data and whose business activity undertakes the relevant processing measure.

"**EEA**" is the European Economic Area (EEA), including the EU member states, Norway, Iceland and Liechtenstein.

"**personal data**" means any information relating to an identified or identifiable natural person, for example names of individuals, contact details, email, phone number and any other information relating to an individual.

"**processing**" means any operation or action performed on personal data, for example collection, recording, storage, adaptation, consultation, use, disclosure, erasure or destruction.

"**profiling**" means automated processing of personal data to "map" personal aspects, such as analysing or predicting health, personal preferences, interests, behaviour, location or movements.

"**registers**" means structured registers of systems and contexts regarding personal data.

"**third country**" is a country outside the EEA, except countries having a data protection level that is considered sufficient by the EU Commission.

## 6. PRINCIPLES FOR PROCESSING OF PERSONAL DATA

Data protection is underpinned by a number of important principles that the Catena Group adheres to.

### 6.1 Lawfulness, fairness and transparency

- Personal data must be processed *fairly and lawfully* (meaning that there must exist a legal basis for the processing and an individual's rights and freedoms must be protected).
- A *fair processing notice* (for example privacy policy and employee privacy notice, and if applicable, cookie policy) regarding the processing of personal data must be provided to individuals whose personal data is being collected and processed. It shall, among other things, clearly set out who the data controller is, the purposes of processing, data subject rights and third parties to whom the personal data may be transferred.
- Catena Media shall maintain a *register* of its processing of personal data in order to fulfil lawfulness, fairness and transparency.

## 6.2 Purpose limitation and data minimisation

- Personal data must be collected only for *specific, explicitly stated and lawful purposes*.
- Personal data must be *adequate* and relevant and not in excess of what is *necessary and proportional* in light of the purposes of the processing (data minimisation). Before new processing of a set of personal data is occurs, Catena Media shall ensure that the processing is compatible with the purpose for which it was originally collected or if not, obtain consent or make sure it satisfies another legal basis (see section 7 below).
- *Privacy by design* and *privacy by default* shall be an integrated part of data processing at the Catena Group. This means that any system, software or technology shall be developed or used in a way that respects the principles of data processing in this section 6. More info on privacy by design and by default is to be found in the Catena Group Privacy by Design and Privacy by Default Procedure.

## 6.3 Accuracy

- Personal data must be accurate and where necessary *kept up to date* and personal data being inaccurate, erased or rectified.

## 6.4 Storage limitation

- Personal data must not be held longer than necessary in light of the purposes of the processing. Personal data shall be *deleted or made anonymous* when there no longer is a legal basis or legal obligation to keep it (including a need for Catena Group to establish or defend its legal rights).

## 6.5 Integrity and confidentiality

- Personal data must be protected by appropriate *organizational and technical measures*, taking into account industry standards, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of individuals. This shall be evaluated at regular intervals.
- *Data protection impact assessments* shall be made before use of a product, service or tool that involves processing of personal data which may potentially present a high risk for rights and freedoms of individuals, especially considering the potential impact and the kind of personal data processed. The assessment shall be recorded in a register. Catena Group's Data Protection Impact Assessment Procedure gives more information in this matter.
- Appropriate technology and operational measures shall be implemented to prevent unauthorized access, illegal processing or distribution, as well as accidental loss, modification or destruction.
- Appropriate back-up and disaster *recovery solutions* shall be in place. Regular testing of systems and protective measures shall be made.
- Access to personal data shall be *limited to personnel who need access for their work*, and appropriate security should be in place to avoid unauthorised sharing of information.
- If a Catena Media company a) is established in the European Union or b) processes personal data about people within the EU, such personal data must not, as a general rule, be transferred

to a third country (unless it ensures an adequate level of protection or appropriate safeguards are in place).

- In the event of a *data breach*, Catena Media shall immediately assess and take measures to eliminate the risk to people's rights and freedoms and, if appropriate, report the data breach to relevant supervisory authority and individuals concerned. All data breaches shall be recorded in a register (also when a data breach is not reported to the supervisory authority/individuals concerned) and handled in accordance with Catena Group's Personal Data Breach Procedure.
- Transmission of personal data to recipients outside the Catena Group must be made based on a legal basis and upon the conclusion of a data processing agreement. The data recipient must be required to use the data only for the defined purposes.
- Transfer of personal data within the Catena Group shall be made in accordance with an *Intra-group data transfer agreement*.
- A *data processing agreement* in writing must be concluded with a third party (processor) who processes personal data on Catena Media's behalf. The processor must be chosen based on demonstrated ability to comply with this Policy and its undertaking to process personal data on Catena Media's instructions only and in accordance with applicable law. When contracting a new third party who processes personal data on Catena Media's behalf, attention shall be given to the rules and procedures found in Catena Group's Choosing and Contracting Processors Procedure.

## 7. DATA SUBJECT RIGHTS

Individuals have certain rights regarding their personal data and any requests for the exercise of such rights shall be dealt with in a timely and transparent manner (normally within one month).

All data subject requests shall be handled in accordance with the Catena Group's Data Subject Access Request Procedure and recorded in a register to allow the Catena Group to submit any information requested by a supervisory authority as well as establish or defend legal rights.

Data subject rights comprise:

◇ *Right of transparent communication and information*

Individuals may request information whether Catena Media holds personal data about him or her, where collected, for what purpose and if transmitted to a third party.

◇ *Right of access*

Individuals have a right to obtain information/copy about personal data processed regarding him or her.

◇ *Right to rectification*

Personal data shall be accurate, and individuals may request changes

◇ *Right to erasure ('right to be forgotten')*

If no legal basis exists for keeping a set of personal data, for example a withdrawn consent, personal data must be deleted unless Catena Media has an overriding legal basis to keep.

◇ *Right to restriction of processing*

if an individual contests Catena Media's processing of personal data, it shall be made unavailable or kept separate depending on the circumstances.

◇ *Right to data portability*

If processing is based on the individual's consent or by contract, personal data of that individual shall be provided in structured, commonly used and machine-readable format

◇ *Right to object*

An individual can object to Catena Media's processing of personal data and that must be respected unless Catena Media can demonstrate that there is a compelling legitimate interest. If the objection pertains to direct marketing and thereto related profiling (see definition in section 2), Catena Media shall immediately stop processing such personal data.

◇ *Right to not be subject to automated decision-making (including profiling)*

If automated decisions are taken by Catena Media and produces legal effects regarding an individual, suitable safeguards shall be in place to allow the individual to be fully informed, respond and request the intervention of an employee at Catena Media.

## 8. LEGAL BASIS

All personal data processed by the Catena Group must be done on one of the following lawful bases:

- *Consent*: the individual has given consent for one or more specific purposes
- *Contract*: as necessary for the performance of a contract with the individual
- *Legal obligation*: necessary for compliance with a legal obligation
- *Vital interest* (of individuals): necessary in order to protect the vital interests (for example medical urgency)
- *Legitimate interest*: necessary for the purposes of the legitimate interests and such interests are not overridden by the interests or fundamental rights and freedoms of the individual

In relation to any processing of personal data, Catena Media shall note the legal basis in the register used for the mapping of personal data processing activities within the Catena Group.

When consent is the legal basis, the individual shall be given clear, concise and specific information about the processing of personal data before giving consent. The granting of consent shall be documented. Further, the individual shall have a right to revoke the consent at any time and appropriate functions and systems shall be in place for that purpose.

## 9. DATA PROTECTION RISKS

This Policy helps to protect the Catena Group from data security risks, including:

- *Breaches of confidentiality.* For instance, information being given out inappropriately or unlawfully.
- *Failing to show transparency.* For instance, Catena Group must be transparent about the processing of personal data carried out in order to ensure that individuals are aware of the processing of personal data relating to them.
- *Reputational damage.* For instance, Catena Group could suffer reputational damage if an unauthorized person or organisation gained access to personal data.
- *Administrative fines, penalty or damages.* As decided by a supervisory authority or a court – maximum fine the higher of 20 000 000 euros or 4 percent of total worldwide annual turnover.

## 10. ROLES AND RESPONSIBILITIES

The Board of Directors is ultimately responsible for ensuring that Catena Group meets its legal obligations.

Each company of the Catena Group is responsible for compliance with this Policy and the national data protection laws applicable to it.

**The GC** is responsible for:

- Keeping the board updated about data protection responsibilities, risks and issues.
- Reviewing all data protection procedures and policies, at regular intervals or as decided in a policy or procedure.
- Arranging data protection training and giving advice to staff, interns, volunteers, consultants and other people working on behalf of Catena Group and covered by this Policy.
- Dealing with data subject rights requests (for example individuals' right to get information about personal data that Catena Media holds about them).
- Approving any contractual arrangement with any third-party services that Catena Media is considering using to process personal data on its behalf (for instance, cloud computing services).

**The Chief Information Officer (CIO)** is responsible for:

- Ensuring all systems, services and equipment used for storing data meet acceptable security standards.

- Performing regular checks and scans to ensure security hardware and software is functioning properly.
- Evaluating any third-party services Catena Media is considering using process personal data on behalf of Catena Group (for instance, cloud computing services).
- Arranging data protection security and integrity training and giving advice to the Relevant Persons.

**All Relevant Persons with managerial responsibilities are responsible for:**

- Informing the GC of any data protection queries from partners, third parties, customers or media outlets.
- Working with the GC to ensure that Catena Group products, marketing initiatives and data, sales data, product data and financial data abide by data protection principles.

All Relevant Persons have a responsibility for ensuring that personal data is collected, stored and handled appropriately and lawfully.

## 11. EXCEPTIONS

There are no exceptions to this Policy. Any need for exceptions to this Policy must be clearly defined and documented. All exceptions shall be approved by the Board of Directors.

## 12. REVIEWS AND UPDATES

The Data Protection Policy shall be reviewed, updated and adopted when deemed necessary or appropriate, however, no less than annually.

The Data Protection Policy shall be reviewed and updated by the General Counsel and adopted by the Board of Directors.

## 13. REFERENCES TO ASSOCIATED DOCUMENTS AND LINKS

- Choosing and Contracting Processors Procedure.
- Data Subject Access Request Procedure
- Data Protection Impact Assessment Procedure
- Personal Data Breach Procedure
- Privacy by Design and Privacy by Default Procedure